



PENSANS COMMUNITY PRIMARY SCHOOL

ONLINE SAFETY POLICY

September 2026 — September 2027

Policy information	Current position
Policy owner	Headteacher / Designated Safeguarding Lead
Designated Safeguarding Leads	Niki Ambrose and Sian Miles
Deputy DSL	Jack Rutterford
Online Safety Lead	Niki Ambrose
Online Safety / Safeguarding Link Governor	Vicky Sanderson
PSHE / RSHE Lead	Niki Ambrose
Computing Lead	Suzanne Earley
Technical support	TPAT IT Support
Data Protection Officer	Judy Brinson, TPAT
Approved by	Local Monitoring Committee / governing body
Approval / review date	September 2026
Next review	September 2027, or earlier where required

1. Policy statement

Pensans Community Primary School is committed to keeping children, staff, governors, volunteers and the wider school community safe when using technology, digital services and online spaces. Online safety is an integral part of safeguarding rather than a separate issue.

The school recognises that online and offline life are closely connected. Harm may begin online, offline or across both environments, and online incidents outside school can affect children's safety, wellbeing, relationships and behaviour in school.

The school will use a whole-school approach combining education, positive relationships, supervision, appropriate filtering and monitoring, effective safeguarding procedures, proportionate behaviour management, staff training, parental engagement, data protection and cyber security.

This policy is intended to be a living document. It will be reviewed at least annually and sooner where legislation, statutory guidance, technology, local context, school systems or emerging risks change.

2. Statutory and guidance framework

This policy should be read alongside the school's safeguarding and operational policies and the following current national framework:

Framework / guidance	Relevance to this policy
Keeping Children Safe in Education 2026 (DfE)	Statutory safeguarding guidance in force from 1 September 2026. Online safety, filtering and monitoring, staff training, safeguarding education and mobile phones are specifically addressed.
Relationships Education, Relationships and Sex Education and Health Education — revised guidance for introduction 1 September 2026 (DfE)	Provides the statutory curriculum context for online relationships, respectful behaviour, wellbeing, harmful content and related safeguarding education.
Meeting digital and technology standards in schools and colleges — Filtering and monitoring core standard (DfE)	Sets current expectations for governance, annual review, checks, filtering, monitoring, reporting, AI-generated content and technical safeguards.
Meeting digital and technology standards in schools and colleges — Cyber security core standard (DfE)	Sets current expectations for cyber risk assessment, secure systems, user accounts, training, updates and resilience.
Teaching online safety in schools (DfE)	Non-statutory curriculum guidance supporting teaching of online safety within existing subjects.
Education for a Connected World — 2020 edition (UKCIS)	Age- and stage-related framework supporting progression in digital knowledge and skills.
Sharing nudes and semi-nudes — updated March 2024 (UKCIS)	Safeguarding response to the creation, sharing and distribution of nude and semi-nude images.
Mobile phones in schools — statutory guidance (DfE, 2026)	Schools should be mobile-phone-free by default and pupils should not have access to mobile phones

	throughout the school day, subject to limited exceptions and reasonable adjustments.
Searching, screening and confiscation in schools (DfE)	Provides the framework for lawful and proportionate searching, including devices and mobile phones.
Preventing and tackling bullying (DfE, current 2026 publication)	Includes prevention and response to bullying and cyberbullying.
Generative artificial intelligence in education (DfE) and Generative AI: product safety standards (DfE)	Provides current expectations for safe, responsible and lawful use of generative AI in education.
Online Safety Act 2023 and Ofcom's protection of children regime	Regulates in-scope online service providers. The school will remain alert to platform-level changes but will not rely on regulation by platforms as a substitute for education and safeguarding.
Data Protection Act 2018, UK GDPR and Data (Use and Access) Act 2025	Provide the data protection framework for personal information, monitoring, images, platforms and information sharing.

3. Aims and objectives

- Promote safe, responsible, respectful and positive use of technology.
- Teach children the knowledge, skills, attitudes and resilience needed to navigate digital life safely.
- Prevent and respond to online harm, including harm occurring outside school that affects children or the school community.
- Ensure children know how and where to report concerns and are confident that adults will listen and act.
- Protect children from illegal, inappropriate and harmful content while avoiding unreasonable over-blocking that prevents legitimate teaching and learning.
- Ensure staff understand their safeguarding responsibilities in relation to online safety, filtering and monitoring, artificial intelligence, digital communications and data protection.
- Maintain clear procedures for responding to cyberbullying, grooming, sexual harassment, sharing of nudes and semi-nudes, harmful content, scams, impersonation, account compromise and other online incidents.
- Ensure technology is used in ways that support inclusion and reasonable adjustments for pupils with SEND or other additional needs.
- Work with parents and carers so that online safety messages are consistent between school and home.
- Review online safety arrangements using evidence from incidents, pupil voice, staff feedback, filtering and monitoring records, curriculum evaluation and changes in national guidance.

4. Scope

This policy applies to all members of the Pensans Community Primary School community, including pupils, teaching and support staff, supply staff, governors, volunteers, contractors, visitors, external providers and parents/carers when using school systems or participating in school activities.

It applies to technology used on school premises, during school trips and events, on school-managed devices used away from school, and to online behaviour outside school where it affects the school community, the safety or wellbeing of pupils or staff, or the orderly running of the school.

5. What we mean by online safety

In line with KCSIE 2026, online risks are considered under four connected areas:

Area	Examples relevant to primary pupils
Content	Pornography; racism; misogyny; antisemitism; self-harm and suicide content; radicalisation and extremism; extreme violence; misinformation, disinformation and conspiracy theories; age-inappropriate games or media.
Contact	Grooming; adults posing as children; harmful peer pressure; coercion; bullying; sexual harassment; exploitation; harmful interactions with generative AI systems.
Conduct	Cyberbullying; sharing or creating explicit images; AI-generated sexual images or deepfakes; impersonation; abusive group chats; recording and sharing fights; doxxing; threats; harmful challenges.
Commerce	Phishing; scams; financial exploitation; inappropriate advertising; gambling-related content; fake competitions, purchases or requests for money.

The school will also consider emerging risks such as generative AI, deepfakes, synthetic media, AI-generated child sexual abuse material, location sharing, livestreaming, recommender systems, account compromise and the manipulation of children through persuasive or addictive design.

6. Roles and responsibilities

6.1 Governing body / Local Monitoring Committee

- Approve this policy and provide strategic challenge and oversight.
- Ensure online safety is embedded within the school's wider safeguarding arrangements.
- Receive assurance that filtering and monitoring are effective, reviewed at least annually and supported by appropriate records.
- Ensure staff receive safeguarding and online safety training and updates.
- Ensure the school considers online safety in curriculum planning, parental engagement, behaviour, safeguarding and risk management.
- Support the school in ensuring that online safety arrangements are proportionate, inclusive and responsive to local context.

6.2 Headteacher / Senior Leadership Team

- Lead implementation of this policy and ensure it is aligned with safeguarding, behaviour, child protection, Prevent, data protection and cyber security arrangements.
- Ensure suitable systems, training, staffing and resources are in place.
- Oversee serious or persistent online safety incidents and ensure appropriate escalation.
- Ensure school systems and policies comply with current DfE standards and statutory guidance.
- Ensure new digital platforms and significant changes to technology are subject to appropriate safeguarding, data protection and security checks.

6.3 Designated Safeguarding Lead / Online Safety Lead

- Take lead responsibility for safeguarding and child protection, including online safety and understanding the school's filtering and monitoring systems.
- Respond to safeguarding concerns identified through disclosures, staff reports, filtering, monitoring or other sources.
- Ensure online incidents are recorded and managed through the school's safeguarding procedures.
- Work closely with TPAT IT Support, senior leaders and the safeguarding governor on filtering and monitoring.
- Maintain awareness of emerging online harms and ensure staff are updated where necessary.
- Ensure children and parents receive appropriate support and information following significant online incidents.
- Review this policy and related acceptable use arrangements annually and after significant changes or incidents.

6.4 TPAT IT Support / technical support

- Maintain filtering, monitoring, network and device protections in accordance with DfE standards and TPAT requirements.
- Work with the DSL and SLT to identify risks, complete checks and respond to technical concerns.
- Provide appropriate monitoring reports and high-risk alerts.
- Ensure systems are updated, supported, secure and configured to reduce opportunities for bypassing safeguards.
- Maintain accurate technical documentation and support cyber incident response.
- Ensure new devices and services are checked before being placed into normal use.

6.5 Online Safety / Safeguarding Link Governor

- Provide strategic challenge and assurance on online safety, filtering and monitoring.
- Meet with the DSL/SLT as appropriate and review evidence of effectiveness.
- Ensure online safety remains part of the governing body's wider safeguarding oversight.

6.6 All staff

- Complete safeguarding and online safety training at induction and receive updates at least annually, with additional updates when required.
- Read and follow the relevant safeguarding, acceptable use, behaviour, staff conduct and data protection policies.

- Report online safety concerns promptly to the DSL/deputy or through the school's safeguarding reporting process.
- Supervise pupils appropriately when they are using technology.
- Model respectful, safe and professional digital behaviour.
- Understand that filtering and monitoring are safeguarding tools and report over-blocking, gaps, bypass attempts or concerning activity.
- Never promise a child confidentiality about a safeguarding concern.

6.7 Pupils

- Use technology safely, respectfully and responsibly.
- Follow the pupil acceptable use agreement and school rules.
- Tell a trusted adult if something online makes them feel unsafe, worried, pressured, threatened or uncomfortable.
- Do not create, share or encourage harmful, humiliating, sexual, threatening or abusive content.
- Respect the privacy, dignity and rights of others.

6.8 Parents/carers

- Support the school's online safety expectations and age-appropriate use of apps, games and social media.
- Report concerns to the school promptly where online activity is affecting a child's safety, wellbeing or school life.
- Use the school's formal communication and complaints routes rather than attempting to resolve school disputes through social media.
- Work with the school following significant incidents and support children to follow age ratings and platform rules.

7. Curriculum and education

Online safety is taught as part of a planned, age-appropriate and progressive curriculum. It is not restricted to a single lesson, subject or annual event.

Key curriculum links include:

- Relationships Education and Health Education / RSHE.
- Computing and digital literacy.
- PSHE and wider personal development.
- Citizenship, where relevant.
- English, media literacy and critical evaluation of information.
- Opportunities arising from current events, pupil questions, incidents and contextual safeguarding information.

Teaching will address, as appropriate to age and development:

- Online relationships, kindness, consent, boundaries and respectful communication.
- Cyberbullying and how to respond to harmful behaviour.
- Privacy, passwords, personal data, location sharing and digital footprints.
- Misinformation, disinformation, fake news, manipulated media and source checking.

- Age ratings, platform terms, privacy settings and parental controls.
- Grooming, coercion, exploitation and how to seek help.
- Sharing images, including the risks and safeguarding implications of nudes, semi-nudes and AI-generated or altered images.
- Pornography and unrealistic representations of relationships, taught in an age-appropriate and safeguarded way.
- Self-harm, suicide, eating disorder content and harmful online communities, with careful signposting and safeguarding.
- Online scams, phishing, financial exploitation and advertising.
- Generative AI, including safe use, critical evaluation, privacy, bias, misinformation, deepfakes and responsible creation of content.
- Healthy digital habits, wellbeing, sleep, balance and managing notifications and screen use.

Curriculum planning will take account of pupils' age, developmental stage, SEND, vulnerability, language needs and the school's local safeguarding context. The school will use the Education for a Connected World framework as a useful progression framework alongside statutory curriculum requirements.

8. Safeguarding concerns and reporting

Online safety concerns are safeguarding concerns. Staff should follow the same safeguarding reporting route whether the concern originates online, offline or across both environments.

Where a pupil discloses an online concern, staff should:

1. Listen calmly and take the concern seriously.
2. Reassure the child that they were right to tell an adult.
3. Avoid blame, shame or judgement.
4. Do not promise secrecy or confidentiality.
5. Do not investigate beyond what is necessary to establish immediate safety.
6. Do not ask the child to forward, display or search for harmful material.
7. Record the concern accurately and promptly.
8. Report to the DSL/deputy in line with the school's safeguarding procedure.

The DSL will determine whether the matter requires pastoral support, behaviour action, early help, referral to children's social care, police involvement, CEOP or another specialist service. Staff should not delay reporting because they are unsure whether an incident is 'serious enough'.

8.1 Staff concerns about another adult

Concerns or allegations about staff, volunteers, contractors or other adults using technology must be managed under the school's safeguarding and staff conduct procedures. A concern about the Headteacher must be reported through the appropriate chair/governing body and Local Authority Designated Officer arrangements.

8.2 Handling safeguarding concerns and incidents

It is vital that all staff recognise that online safety is an integral part of safeguarding and child protection. Online risks should be considered alongside all other safeguarding concerns, as required by **Keeping Children Safe in Education (KCSIE)**. Online safety includes protecting children from harmful content, contact, conduct and commercial risks, as well as exposure to cyberbullying, child-on-child abuse, online

grooming, extremism, misinformation, disinformation, deepfakes and other emerging technologies, including artificial intelligence (AI). [\[gov.uk\]](https://www.gov.uk), [\[rghs.org.uk\]](https://www.rghs.org.uk)

General concerns must be handled in the same way as any other safeguarding concern. Safeguarding is often described as a jigsaw puzzle, and all stakeholders should err on the side of sharing information with the Designated Safeguarding Lead (DSL), Deputy DSL or Online Safety Lead. Individual concerns may appear insignificant in isolation but could contribute to a wider safeguarding picture. [\[gov.uk\]](https://www.gov.uk)

Support staff often have unique opportunities to identify concerns in playgrounds, corridors, dining areas, transport, extracurricular activities and online environments. Staff should remain alert to indicators of bullying, cyberbullying, child-on-child abuse, sexual harassment, sexual violence, harmful sexual behaviour, exploitation and other safeguarding concerns. [\[gov.uk\]](https://www.gov.uk), [\[assets.pub...ice.gov.uk\]](https://assets.publishing.service.gov.uk)

The school's procedures for dealing with online safety concerns are detailed within the following policies and documentation:

- Safeguarding and Child Protection Policy
- Child-on-Child Abuse Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Acceptable Use Agreements (AUPs)
- Remote Learning Policy
- Data Protection and Information Security Policies
- Filtering and Monitoring Policy and Procedures
- Cyber Security Policy
- Prevent Risk Assessment and Policy
- Relationships, Sex and Health Education (RSHE) Policy
- Mobile Phone and Smart Device Policy
- Social Media Policy

The school is committed to taking all reasonable precautions to safeguard children online. However, it is recognised that online incidents may occur both within and beyond the school environment and can have a significant impact on pupils' safety, wellbeing and education. All members of the school community are encouraged to report concerns promptly so that they can be addressed quickly, appropriately and sensitively. [\[gov.uk\]](https://www.gov.uk), [\[assets.pub...ice.gov.uk\]](https://assets.publishing.service.gov.uk)

Any suspected online risk, safeguarding concern, cyber security incident or breach of acceptable use should be reported immediately to the DSL, Deputy DSL or Online Safety Lead. Where the concern presents an immediate safeguarding risk, staff must act without delay and follow child protection procedures. All concerns should be recorded in accordance with the school's safeguarding procedures. [\[gov.uk\]](https://www.gov.uk)

The school maintains appropriate filtering and monitoring systems to support safeguarding. Staff should be aware that filtering and monitoring are not a replacement for active supervision, education and effective safeguarding practice. Concerns identified through filtering and monitoring systems should be reviewed and escalated where appropriate. [\[gov.uk\]](https://www.gov.uk), [\[oursafersc...ools.co.uk\]](https://www.oursaferschools.co.uk)

Any concern or allegation regarding staff conduct, professional boundaries, misuse of technology, inappropriate online behaviour or unsafe use of school systems must be reported immediately to the Headteacher. Concerns relating to the Headteacher must be referred to the Chair of Governors (or Proprietor) and the Local Authority Designated Officer (LADO). Staff may also use the NSPCC Whistleblowing Advice Line where appropriate. [\[gov.uk\]](https://www.gov.uk)

The school will work with external agencies where necessary, including:

- Local Authority Safeguarding Partners
- Local Authority Designated Officer (LADO)
- Police
- Children's Social Care
- UK Safer Internet Centre Professionals Online Safety Helpline (POSH)
- National Crime Agency (NCA) CEOP
- Internet Watch Foundation (IWF)
- Prevent Education Officers
- Regional Cyber Crime Units
- Other specialist safeguarding services

The DfE's **Behaviour in Schools: Advice for Headteachers and School Staff (February 2024)** should be used alongside safeguarding procedures when responding to online behaviour incidents, child-on-child abuse, sexual harassment, sexual violence, misuse of mobile devices and behaviour occurring online but impacting the school environment. [\[assets.pub...ice.gov.uk\]](https://assets.publishing.service.gov.uk), [\[gov.uk\]](https://www.gov.uk)

Parents and carers will normally be informed of online safety incidents involving their children unless doing so would place the child at increased risk of harm. The school will involve the Police and other agencies where behaviour may constitute a criminal offence or present a significant safeguarding concern. Specific procedures are in place for incidents involving nude or semi-nude image sharing, sexual harassment, sexual violence, online exploitation and harmful sexual behaviour. [\[gov.uk\]](https://www.gov.uk), [\[assets.pub...ice.gov.uk\]](https://assets.publishing.service.gov.uk)

The school will regularly review safeguarding reporting arrangements to ensure they remain effective during periods of remote education, emergency closure, disruption or unusual operating circumstances. Alternative reporting routes will be communicated where required. [\[gov.uk\]](https://www.gov.uk)

9. Specific online safeguarding incidents

9.1 Sharing nudes and semi-nudes

- The school uses the current UKCIS/DfE terminology 'sharing nudes and semi-nudes'.
- This includes photographs, videos, livestreams and digitally altered or AI-generated sexual images involving under-18s.
- A member of staff who becomes aware of an incident must report immediately to the DSL/deputy and must not forward, save, copy or deliberately view an image.

- The DSL will follow the current national guidance, assess risk, support the child and determine whether other agencies need to be involved.
- The school will avoid language that blames, shames or criminalises a child who has been harmed or coerced.

9.2 AI-generated sexual images / deepfakes

AI-generated or digitally altered sexual images involving children are treated as a serious safeguarding matter. The fact that an image is synthetic, edited or 'not real' does not remove the potential for significant harm. The school will follow KCSIE 2026 and current specialist safeguarding guidance.

9.3 Cyberbullying and harmful online behaviour

- Cyberbullying will be managed under the school's Behaviour and Anti-Bullying Policies as well as this policy.
- Online behaviour outside school may be addressed where it causes harm, affects pupils or staff, or has a clear impact on the school environment.
- The school will consider repeated low-level incidents, group behaviour, exclusion from online groups, impersonation, sharing humiliating material and 'banter' that causes harm.
- The school will support the child experiencing harm and address the behaviour and underlying needs of the child who has caused harm.

9.4 Child-on-child sexual harassment and sexual violence

Online sexual harassment, sexual violence, sexualised messaging, coercion, sharing sexual material and related conduct are safeguarding matters. Staff must report concerns to the DSL, who will follow KCSIE 2026, the child protection policy and the school's child-on-child abuse procedures.

9.5 Grooming, exploitation and inappropriate contact

Any concern that an adult or another child is attempting to groom, exploit, manipulate, threaten or coerce a pupil online must be reported immediately to the DSL/deputy. This includes contact through games, social media, messaging apps, livestreams, educational platforms and generative AI systems.

9.6 Harmful challenges, hoaxes and disturbing content

The school will respond to harmful online challenges, hoaxes or viral content proportionately and without unnecessarily amplifying harmful material. Parents/carers will be informed where appropriate and curriculum or pastoral responses will be used where a wider group of pupils has been affected.

10. Filtering and monitoring

Filtering and monitoring are distinct safeguarding functions. Filtering aims to prevent access to illegal, inappropriate and potentially harmful content. Monitoring identifies and alerts the school to concerning activity; monitoring does not itself prevent access.

Current school arrangements include:

Area	Pensans arrangement
Filtering	Netsweeper On Guard is used for school internet access and school-managed devices, including

	devices used away from school where the technical configuration supports this.
Filtering management	Changes are managed by authorised school/TPAT personnel in line with safeguarding and technical procedures.
Monitoring	The school uses a combination of direct staff supervision, network monitoring/logs and individual device monitoring through appropriate software/services.
Technical support	TPAT IT Support, working with the DSL/SLT.
Safeguarding responsibility	The DSL leads the safeguarding response to alerts and concerns; governors/SLT provide strategic assurance.

The school will ensure that:

- Filtering and monitoring provision is reviewed at least annually and sooner where there is a significant safeguarding, technology or working-practice change.
- The review considers pupil age, SEND, EAL, risk profile, technology use, AI tools, BYOD arrangements, incidents and the curriculum.
- Checks are completed and recorded at a frequency appropriate to the school's risk profile.
- High-risk safeguarding, technical or malicious incidents are escalated promptly.
- Filtering is applied appropriately to school-managed devices and networks, including devices used away from school where applicable.
- Safe search is enabled and technical protections against bypassing safeguards are maintained.
- Staff know how to report unsuitable content, over-blocking, gaps, bypass attempts and failures in filtering or monitoring.
- Temporary exceptions to filtering/monitoring are authorised, risk assessed and recorded.
- Monitoring and filtering data is handled in accordance with data protection requirements, with appropriate DPIAs and privacy information where required.
- The school recognises that no technical system is 100% effective and therefore combines technical controls with education, supervision and professional judgement.

11. Artificial intelligence (AI)

The school recognises that generative AI is now part of the digital environment in which children and staff live and learn. The school will use AI cautiously, safely and educationally, with safeguarding, data protection, intellectual property and developmental considerations at the centre.

11.1 School use of AI

- Only school-approved AI tools may be used for school business, teaching or pupil-facing activity.
- New AI tools must be considered through the school's technology approval, safeguarding, data protection and cybersecurity processes.

- Personal, confidential or safeguarding information must not be entered into public or unapproved AI systems.
- Staff must check AI-generated content for accuracy, bias, age appropriateness, safeguarding concerns and copyright/intellectual property issues.
- AI output must not replace professional judgement, teacher assessment or safeguarding decision-making.
- Where an AI tool is pupil-facing, the school will consider age appropriateness, filtering, monitoring, privacy, data processing, developmental risks and the supplier's safety arrangements.
- Pupils will be taught that AI can produce false, biased, manipulative or inappropriate information and that they must think critically about its output.
- The school will address the risks of deepfakes, impersonation, manipulated images and synthetic sexual content through age-appropriate teaching and safeguarding.

11.2 Pupil use of generative AI

- Pupils may only use generative AI where the teacher or school has explicitly permitted it for an educational purpose.
- Pupils must not use AI to create sexual, violent, threatening, humiliating or discriminatory material.
- Pupils must not use AI to impersonate another person or create harmful images or messages about another pupil, staff member or member of the community.
- Pupils should not share personal information, passwords, photographs or sensitive information with AI systems.
- Where AI is used in assessed work, pupils must follow the teacher's instructions about acknowledgement and originality.

12. Approved communication and online platforms

The school currently uses the following authorised systems for communication and learning:

System	Primary purpose / expectation
Common sense media	Pupil digital learning and online safety education; centrally managed.
Showbie	Learning and communication; centrally managed.
Microsoft Outlook	Official staff email. Staff must not use personal email accounts to communicate with pupils or for school/child data.
ARBOR	Authorised school communication and school/child data functions.
Other platforms	Must be approved in advance through school/TPAT processes and appropriately managed.

Any new platform that enables communication, child logins, storage of school/child data, AI interaction or public sharing must be approved before use by the appropriate school/TPAT personnel, including data protection and technical checks where required.

Staff must not use personal/private messaging accounts or unapproved apps to communicate directly with pupils. Where an accidental use of a personal account occurs, the incident must be reported immediately to the Headteacher/DSL/DPO as appropriate.

13. Digital images, video and livestreaming

- The school will use image/video permissions and information held in ARBOR or the school's current consent system when deciding whether an image may be used for a stated purpose.
- Staff must check current permissions before using images for public-facing purposes.
- Public-facing pupil material should use only the minimum identifying information necessary and should not disclose sensitive personal information.
- Staff must follow the school's data protection policy and retention arrangements when storing images and video.
- Personal devices should not be used to store pupil images or data except where explicitly permitted by school policy and only for the shortest period necessary before secure transfer and deletion.
- Staff, pupils, parents and visitors must not livestream, photograph or record children without appropriate permission and in accordance with school arrangements.
- Pupils are taught about consent, privacy, location information, digital footprints and the risks of sharing images of themselves or others.

14. Social media and online reputation

The school recognises that social media is part of modern life. All members of the school community are expected to communicate respectfully and not post material that is threatening, abusive, discriminatory, defamatory, bullying, unlawful or likely to cause safeguarding harm.

- Parents/carers should use the school's official communication and complaints procedures rather than attempting to resolve school disputes through social media.
- Pupils must not use social media or other online services to bully, threaten, impersonate or harass other pupils or staff.
- Staff must maintain professional boundaries and must not communicate with pupils through personal social media accounts.
- Staff should avoid posting material that could reasonably be attributed to the school or profession in a way that undermines trust or safeguarding.
- Pupils and staff should not accept inappropriate friend/follow requests or use social media to bypass school communication systems.
- The school may take proportionate action in response to online behaviour outside school where it affects pupil safety, staff wellbeing or the orderly running of the school.

15. Mobile phones, smart watches and personal devices

From 1 September 2026 the school follows the DfE statutory guidance that schools should be mobile-phone-free environments by default. Pupils should not have access to mobile phones throughout the school day, including lessons, transitions, breaktimes and lunchtime, except where an agreed exception or reasonable adjustment applies.

The exact storage, collection and sanctions arrangements are set out in the school's current Mobile Phone / Behaviour Policy and will be applied consistently.

- Pupils must not use mobile phones, smart watches or other communication devices during the school day unless an authorised exception applies.
- Any exception for medical, SEND, accessibility, safeguarding or other exceptional reasons must be agreed by the school and managed safely.
- Staff must follow the staff acceptable use arrangements for personal devices.
- Staff should not use personal phones in front of pupils except where specifically permitted for an appropriate school purpose or in an emergency.
- Volunteers, contractors, governors and visitors must follow the school's arrangements for personal devices and photography.
- Parents/carers should not contact pupils directly on personal devices during the school day; urgent messages should go through the school office.

16. School devices, remote learning and trips

- School devices remain subject to school policies whether used on site or away from school.
- Devices used at home should be treated as school devices and used in accordance with the same safeguarding and acceptable use expectations.
- Teachers supervising online learning or remote activities must use approved platforms and follow safeguarding and professional boundaries.
- On trips and off-site activities, staff should use the school's duty phone or other authorised communication arrangements wherever provided.
- Any deviation from approved communication arrangements, including emergency use of a personal phone, should be reported to the Headteacher as soon as practicable.

17. Searching, confiscation and access to devices

Searching and confiscation will be carried out in accordance with current DfE guidance, the school's Behaviour Policy, Mobile Phone Policy and relevant legislation.

- Only the Headteacher or staff authorised in accordance with the school's procedures may exercise search powers.
- Any search must be lawful, necessary and proportionate and take account of pupil age, SEND, vulnerability and individual circumstances.
- Where a device is searched, staff must follow the school's procedures for handling digital content and safeguarding concerns.
- If staff encounter suspected illegal or safeguarding material, they must preserve safety and evidence and seek advice from the DSL/police as appropriate rather than circulating or copying material.
- Nudes or semi-nudes must not be deliberately viewed, copied, forwarded or stored by staff who are not required to do so as part of a lawful safeguarding/technical process.
- Confiscated devices must be handled securely and returned or retained in line with the school's current behaviour and mobile phone arrangements.

18. Data protection and privacy

Online safety and data protection are closely connected. The school will process personal information lawfully, fairly and transparently and will apply data protection principles to online platforms, images, communications, filtering, monitoring and AI.

- The school will maintain appropriate privacy notices and data protection documentation.
- Where required, the school will complete Data Protection Impact Assessments for monitoring systems, AI tools and other high-risk processing.
- Staff will only use approved systems for school and child data.
- Passwords and authentication credentials must be kept secure and must not be shared.
- Personal information will only be shared where there is a lawful basis and in accordance with safeguarding and information-sharing requirements.
- Data protection law must not be used as a reason to prevent appropriate safeguarding information sharing where there is a lawful basis to share.
- The school will follow its retention schedule and securely dispose of information when it is no longer required.

19. Cyber security

Cyber security is part of safeguarding. The school will work with TPAT IT Support to maintain secure, resilient systems and reduce the risk of cyber incidents affecting children, staff, learning or sensitive data.

- The school will conduct a cyber risk assessment at least annually and revisit it termly, and following significant changes or incidents.
- User accounts will be appropriately controlled and access limited to what is required for the user's role.
- Security updates and supported software will be maintained.
- Multi-factor authentication will be used where required and available for appropriate systems.
- Backups, recovery and business continuity arrangements will be maintained through TPAT processes.
- Staff will receive appropriate cyber security awareness training and know how to report suspected phishing, malware, data breaches or other incidents.
- Suspected cyber incidents must be reported immediately through the TPAT/school incident route and, where relevant, to the DPO/DSL.

20. School website and public-facing information

- The school website is a public-facing communication channel and must be maintained in accordance with current statutory requirements.
- Content must be accurate, appropriate, accessible and reviewed.
- Copyright, licensing and permissions must be respected.
- Pupil information and images must be published only where authorised and appropriate.
- Staff should seek SLT advice where there is uncertainty about copyright, safeguarding, privacy or publication.

Current website arrangements: the site is hosted by E-Schools; day-to-day content responsibility sits with the school/SLT as currently delegated.

21. Parents, carers and the wider community

The school will support parents/carers to understand online risks and promote safe digital habits. Communication will be proportionate and age-appropriate.

- The policy will be published on the school website.
- Online safety information will be reinforced through newsletters, meetings, workshops or signposting where appropriate.
- Parents/carers will be informed about the school's filtering and monitoring arrangements and the online platforms pupils are expected to use.
- Parents/carers will be encouraged to use age ratings, parental controls, privacy settings and family agreements.
- The school will signpost families to reputable support, including CEOP, Childline, Internet Matters, Childnet, UK Safer Internet Centre and other relevant services.

22. Staff training and professional development

- Online safety will form part of safeguarding induction for all staff, including temporary, supply and support staff.
- All staff will receive safeguarding and online safety updates at least annually and whenever significant new risks or requirements emerge.
- Training will include staff responsibilities for filtering and monitoring.
- Staff will receive appropriate updates on generative AI, deepfakes, image-based abuse, cyber security, scams, online sexual harassment and emerging risks.
- Governors will receive appropriate safeguarding and online safety training and updates so they can provide effective strategic challenge.
- Training will reflect the needs of pupils with SEND and other vulnerabilities.

23. Recording, monitoring and review

Online safety incidents and concerns will be recorded in the school's safeguarding, behaviour, technical or other appropriate systems. Records will enable leaders to identify patterns, repeat incidents, vulnerable groups, locations, platforms, times and the effectiveness of interventions.

The school will review:

- Safeguarding and behaviour incident records.
- Filtering and monitoring reports and checks.
- Cyber security incidents and near misses.
- Pupil voice and staff feedback.
- Curriculum coverage and pupil understanding.
- Parent/carers feedback and emerging concerns.
- Changes in technology, platforms, AI and online harms.
- Changes to legislation, statutory guidance and DfE standards.

The policy will be reviewed at least annually. An earlier review will take place where there is a significant change in legislation, statutory guidance, technology, school systems, local context or safeguarding risk.

24. Related school policies and procedures

- Child Protection / Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- Mobile Phone Policy / Behaviour arrangements
- Acceptable Use Policies for staff, pupils and parents/carers
- Staff Code of Conduct / Staff Behaviour Policy
- RSHE / Relationships Education Policy
- Computing Policy
- Data Protection / Privacy Policy
- Cyber Security arrangements / TPAT cyber procedures
- Prevent Risk Assessment / Policy
- Complaints Policy
- SEND Policy
- Image / photography consent arrangements
- Information sharing and record retention procedures

25. Minimum response pathway for online safety concerns

Stage	Action
1. Notice or disclosure	A child, staff member, parent/carers or technical system identifies a concern.
2. Immediate safety	If there is immediate danger, take reasonable action to keep the child safe and seek emergency assistance where required.
3. Report	Report to the DSL/deputy using the school's safeguarding route. High-risk filtering/monitoring alerts are escalated promptly.
4. Do not investigate unnecessarily	Do not forward, copy, deliberately view or ask a child to display harmful material. Preserve information only where authorised and necessary.
5. DSL assessment	The DSL assesses safeguarding, pastoral, behaviour, technical and legal considerations and decides whether further referral is required.
6. Multi-agency action	Where appropriate, the DSL refers to children's social care, police, CEOP or another specialist service and works with them.
7. Support	Support the child and others affected, including pastoral, SEND, mental health or family support where appropriate.
8. Record and review	Record the incident and outcome, identify patterns and consider whether curriculum, supervision, filtering, monitoring, training or policy changes are required.

26. Current school-specific technical and communication arrangements

Arrangement	Current Pensans position
Internet filtering	Netsweeper On Guard
Technical support	TPAT IT Support
Pupil learning / communication	Teach Computing/Common Sense Media/Lifewise
Staff email	Microsoft Outlook
Parent / school data communication	ARBOR
Website host	E-Schools
Online Safety Lead	Niki Ambrose
DSLs	Niki Ambrose and Sian Miles
Deputy DSL	Jack Rutterford
Safeguarding / Online Safety Link Governor	Vicky Sanderson
PSHE / RSHE Lead	Niki Ambrose
Computing Lead	Suzanne Earley
DPO	Judy Brinson, TPAT

27. Review record

Date	Action	Next review
September 2026	Full policy refresh. Removed obsolete 2022/2023/2024 references; updated KCSIE, RSHE, mobile phone, filtering/monitoring, cyber security, AI and current online harms; retained relevant Pensans arrangements.	September 2027

This policy should be reviewed sooner if there are changes to legislation, statutory guidance, DfE digital standards, safeguarding requirements, school systems, TPAT arrangements or significant emerging online risks.

Appendix A — Current reference list

- **Department for Education** — Keeping children safe in education 2026 — statutory guidance, in force from 1 September 2026.
- **Department for Education** — Relationships Education, Relationships and Sex Education and Health Education — revised statutory guidance for introduction 1 September 2026.
- **Department for Education** — Meeting digital and technology standards in schools and colleges — Filtering and monitoring: core standard.
- **Department for Education** — Meeting digital and technology standards in schools and colleges — Cyber security: core standard.
- **Department for Education** — Teaching online safety in schools.
- **UK Council for Internet Safety** — Education for a Connected World — 2020 edition.
- **UK Council for Internet Safety / DfE** — Sharing nudes and semi-nudes: advice for education settings working with children and young people — updated March 2024.
- **Department for Education** — Mobile phones in schools — statutory guidance, effective from 1 September 2026.
- **Department for Education** — Searching, screening and confiscation in schools.
- **Department for Education** — Preventing and tackling bullying — current publication, updated July 2026.
- **Department for Education** — Generative artificial intelligence (AI) in education — current guidance.
- **Department for Education** — Generative AI: product safety standards — updated January 2026.
- **Ofcom** — Online Safety Act — protection of children duties and codes of practice.
- **Information Commissioner's Office** — Age appropriate design: a code of practice for online services / Children's Code.
- **Legislation** — Data Protection Act 2018; UK GDPR; Data (Use and Access) Act 2025.

Key online sources

- <https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>
- <https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education>
- <https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-core-standard>
- <https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-core-standard>
- <https://www.gov.uk/government/publications/mobile-phones-in-schools/mobile-phones-in-schools>
- <https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people>
- <https://www.gov.uk/government/publications/generative-artificial-intelligence-ai-in-education>
- <https://www.gov.uk/government/publications/generative-ai-product-safety-standards>